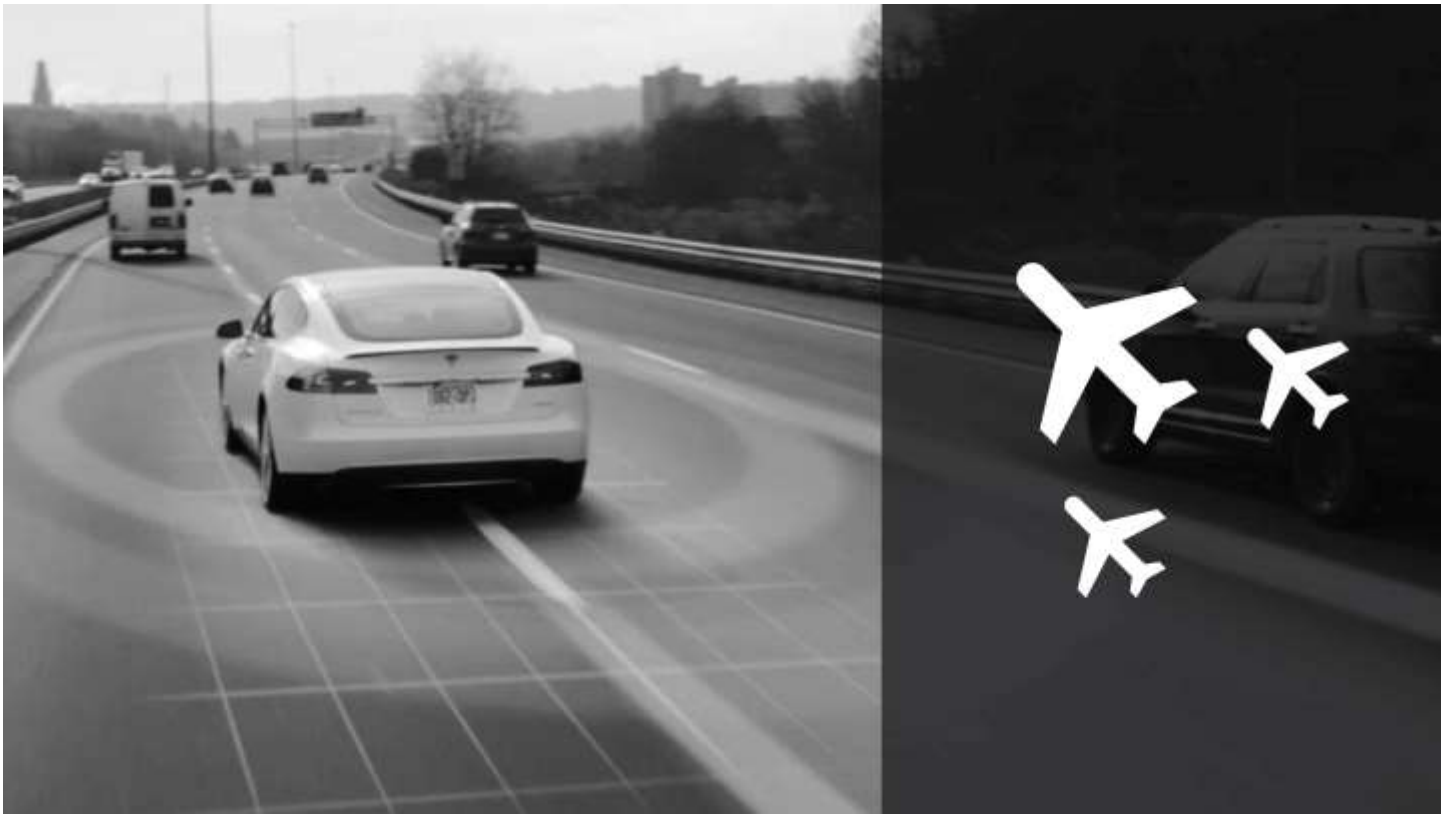
Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification



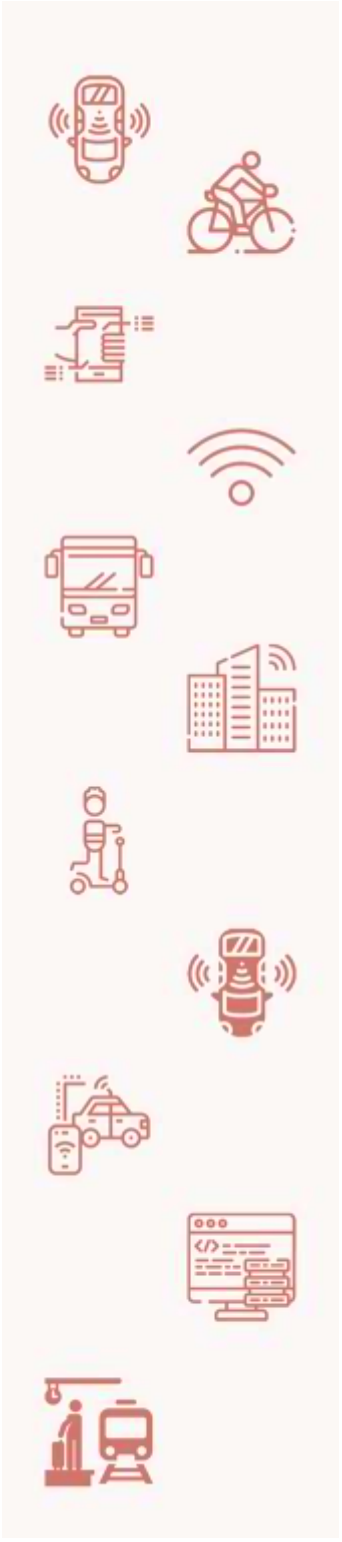
How can transportation agencies leverage certification lessons learned from the aviation industry for roadworthiness assessments and safe deployment of automated vehicles?

Imagine flying across the country knowing that every state regulates airworthiness using different and inconsistent standards. This is the scenario that currently awaits developers of automated vehicles (AV). AVs have tremendous potential to reduce congestion, increase efficiencies leading to reduced energy consumption, and increase productivity through multitasking. Despite the widespread testing and pilot deployment of AVs among private and academic agencies, many unknowns remain. Without consensus, AVs are difficult to regulate, including a lack of national standards for vehicles, licensing regulations, and insurance, and a limited understanding of the roles and responsibilities that will change with deployment of AVs. Texas has the potential to further the development of AVs through regulatory actions targeted at ensuring the safety of roadway users.

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification



KEY STRATEGIES

01

Facilitate Creation of a Central Set of Safety Principles

A central set of safety principles governing the safety assessment and ultimately the certification of AVs provides a mechanism to ensure the safe deployment of AVs onto public roads.

02

Encourage Public/Private Collaboration

Open dialogue between the public and private interests is needed during the certification process to properly evaluate the safety impacts of major changes to systems.

03

Leverage Continuous Reviews of Standards and Assessment Processes

As technology continuously improves and becomes increasingly powerful, regular reviews of vehicle standards are needed to cover new and emerging technology in a proactive rather than reactive process.

04

Consider Public Outreach and Consumer Education

Consumer education and public outreach on how AVs and their systems function allows for the public to better react to adverse operations while riding or driving an AV.

05

Work with Governor's CAV Task Force on AV Safety

Increased deployments of AV pilots will require a unified approach to safety; thus, various task forces within Texas should work together to promote a set of safety standards.

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification

INTRODUCTION

As the number of autonomous vehicle (AV) testing and pilot programs have increased over the last decade, several high-profile crashes and mishaps have occurred, creating some level of distrust in vehicle automation. To promote technological innovation and encourage all the emerging technologies, no standards have been created specifically to oversee and ensure the safety of vehicles with automated features. Currently the Federal Motor Vehicle Safety Standards (FMVSS) serve as the primary standards used to regulate all vehicles.

To understand the complexity of the validation and certification process for automated transportation technologies, researchers and policymakers can gain insights from the aviation industry. Regulatory agencies—first the Civil Aeronautics Authority (CAA) and then the current Federal Aviation Administration (FAA)—have been issuing safety certificates to aircraft since 1938. Over those 80 years plane automation has increased significantly, with the FAA adapting and creating standards and testing procedures for the certification of airworthiness of these planes. As the amount of automation within vehicles continues to increase, the automobile industry can look to lessons learned from aviation in order to develop safety standards and validation/certification procedures to ensure the safe operation of AVs. Amongst the most impactful developments within the aviation industry have been:

1. The creation and compilation of a **uniform set of airworthiness standards**. Having these uniform sets of standards allows for a known certification process, ensuring the safety of aircraft and those flying within them. Having a set of worthiness standards in place for AVs can increase the public trust of automation in on-road vehicles. AVs will need to be certified as safe vehicles, whether through a voluntary process at the point of manufacture, as is currently the case with the FMVSS program, or through a mandated process during vehicle development, as is employed in the aviation industry.
2. The need to **review the certification process** for modified versions of already certified designs. When a new plane design varies only slightly from a previous design, the manufacturer may obtain an amended certificate of airworthiness rather than a new certification, which allows for a reduced testing and validation timeline (3 to 5 years versus 5 to 9 for new aircraft). While this is a common process in other industry sectors (for example, in the medical device community), it has its drawbacks, which were highlighted by the recent Boeing 737 MAX design faults. The 737 crashes serve as a cautionary tale about issues that may arise with AV roadworthiness certifications when applying the traditional FMVSS to emerging technology, particularly given the increased number of automotive recalls in the last 20 years.
3. **Clear roles and responsibilities** of those involved within the certification process. As the aviation industry grew and developed, the FAA and its predecessors took a hands-on role in the certification and inspection of aircraft in order to ensure the safety and continued commerce of US airways. To ensure that certification is handled in a timely manner, the FAA can delegate to qualified individuals or organizations the ability to conduct certain activities on their behalf.

As Texas law does not require that those operating AVs on public roads disclose their vehicle as an AV, we do not know how many AVs are currently on

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification

Texas roads. As Ford, Waymo, TuSimple, and other companies are deploying and testing AVs within Texas, the Texas Department of Transportation (TxDOT) needs to stay informed on the regulatory barriers that are endemic to AVs. With the recent creation and kickoff of the Governor's Connected and Autonomous Vehicle (CAV) Task Force, state transportation officials need to be aware of the current processes used to assess and certify motor vehicles for safety. The lessons learned from aviation can provide insights on incorporating automation into these processes as well as valuable information for agencies involved in the creation of a balanced and flexible regulatory framework that will ensure the safety of AVs, while allowing for innovation and progress.

HISTORY OF AVIATION CERTIFICATION

The federal government has been involved in the development and governance of the US aviation industry since the Air Commerce Act of 1926, when the federal government was given the mandate to foster air commerce[1]. This was achieved through the designation of airways; establishment, maintenance, and operation of navigational aids; airworthiness certificates for aircraft and major aircraft components; and accident investigation. Under the governance of the Commerce Department, the first airworthiness inspections of aircraft began in 1927, with the first *type certificate* (design approval) being issued. The decision in the case of United States v. Drumm in 1944 further strengthened the federal government's role in governing the public airspace, upholding federal authority to require certification of every pilot and aircraft using US airspace[2].

Through discussions with the Department of Justice, the CAA, and the National Association of State Aviation Officials, principles governing federal-state relationships were agreed upon in 1946. Amongst the agreements was that the CAA would continue to enforce regulations concerning airworthiness of aircraft, competency of airmen, operating standards, and air traffic rules[2]. The state aeronautical boards were to administer punishment for those operating recklessly within their jurisdictions, with states having the authority to adopt their own safety standards as long as they were not in conflict with federal rules. Another step the CAA took in 1946 was to create regional offices to handle the increasing requests for certificates, rather than issuing all certificates from Washington[2], in order to mitigate any certification-related delays for aircraft manufacturers.

After its creation in 1958, the FAA authorized the establishment of delegate authority to certify helicopters, small turbine engines, and aeronautical parts for qualified manufacturers. The FAA furthered this authorization with the creation of Designated Alteration Stations by qualified manufacturers, air carriers, commercial operators of large aircraft, and domestic repair stations. Through these acts, the FAA entered a new era of increased industry participation within the certification process of aeronautical products, including aircraft and aircraft parts. The FAA also went on to establish the Office of Airworthiness and passed an emergency rule on the experience requirement for commercial pilots in the wake of several fatal crashes in which the pilots were not experienced enough to take over flight operations from the autopilot.

Under the governance of the Commerce Department, the first airworthiness inspections of aircraft began in 1927, with the first type certificate being issued.

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification

Aviation Automation

Recognizing the complexity of flying, autopilot systems were under development within a decade after the Wright brothers' first flight. The first of these systems to become widely popular was the "gyroscopic automatic pilot" developed by Lawrence Sperry. Sperry's invention, rising to popularity in the 1920s and 1930s, allowed for the automatic balance and straight flight of planes. Using arguments similar to those used by proponents of AVs (that most crashes and incidents were due to human error), digital automation for planes was introduced in the 1970s. The digital autopilots operated using fly-by-wire methods, in which an action was prompted by the pilot. For example, pulling back on the control stick informs the computer that the pilot wants to pitch the plane, at which point the autopilots determine the proper pitch and speeds. These fly-by-wire systems were fully adopted by airlines and manufacturers by the 1980s and 1990s[3]. While automation can perform many flight tasks, the FAA has placed restrictions on the use of automation during take-off and landing maneuvers—with a mandate that pilots control planes beneath 500 ft, leading to 99% of landings being manual[4].

A type certificate is a design approval issued by the FAA once an aircraft complies with all applicable regulations.

As with the automation of any system, the automation of aviation functions had a number of advantages and disadvantages. One of the most significant benefits of automation to the aviation industry was the reduction in workload in the cockpit; as the autopilots took over repetitive functions, the human pilots could focus on other tasks. This reduced workload also decreased the number of personnel in the cockpit from five to two, as only the pilots' presence was now required. In addition to decreasing the workloads for pilots, autopilots provide the advantage of being able to analyze and react to changes in flight controls quicker than a human pilot can, which reduces the effects of weather and increases passenger comfort. Lastly, autopilots have the benefit of providing enhanced system monitoring and diagnostics—allowing for increased understanding of system performance and reliability[5].

However, the automation of tasks within the aviation industry was accompanied by unforeseen disadvantages. Some fatal crashes in the 1990s were attributed to over-reliance on automation, as the pilots lacked sufficient experience in manual flight to take over when the autopilots could not operate as intended. In response, the FAA enacted policies that required a certain number of hours of manual flight each month for pilots, ensuring that their flight skills do not deteriorate.

As AVs are still in development, with full automation not expected in the near future, understanding the role the driver has at each automation level is essential for safe operation. Although AVs can perform lane keeping, and other basic driving functions, over reliance by drivers on this automation can lead to adverse operations. Until AVs reach the level of full automation, drivers will need to maintain situational awareness and the skills needed to takeover control of the AV should they be prompted to do so.

Current Certification Process

The current process for aviation certification and airworthiness, overseen by the FAA, was approved by Congress in 2018 with the FAA Reauthorization Act. As defined by the FAA, a type certificate is a design approval issued by the FAA once an applicant demonstrates that a product (aircraft) complies

with all applicable regulations[6]. The type certificate is the first step to other FAA approvals, such as production and airworthiness certificates. During this stage of certification, the applicant develops a certification plan and timeline to show how they will meet applicable standards. The certification process is overseen by the FAA from the initial conceptual design to post-certification activities, such as summary reports and data retention. Figure 1 shows the typical certification process, and provides the corresponding Texas state agency that might administer each stage of the process.

Per §44704(6)(c) and §44704(6)(d) of the US Code, *production certificates* shall be authorized for the production of duplicates of an aircraft for which a type certificate has been issued, while *airworthiness certificates* shall be issued when the aircraft is found to conform to its type certificate and, after inspection, is in condition for safe operation[7] (49 U.S.C. §44704, 2018). *Condition for operation* refers to the initial determination by the FAA, or an authorized representative, that the condition of the aircraft is conducive to safe operations. To determine if an aircraft meets the condition for operation, inspectors will evaluate items such as aircraft make, model, age, type, and overall condition of the aircraft[8]. Provided by the FAA, *Order 8110.4C, Type Certification* outlines the process and the steps involved in obtaining a type certificate. Figure 2 shows the V-model typically used in systems engineering and how the model can be applied for aircraft systems verification and certification[9].

Translating the aircraft certification process to road vehicles, such as AVs, can be accomplished by including the appropriate regulators at each step in the process (as illustrated in Figure 1). As an example, for the design phase of the review process, the National Highway Traffic Safety Administration (NHTSA) and the Federal Motor Carrier Safety Administration (FMCSA) could work together to oversee AV design, as they oversee the federal governments vehicle and truck safety standards. As they oversee operations and construction of the US highway system, the Federal Highway Administration could also work with FHWA and

Figure 1: Application of the Aircraft Certification Process to Road Vehicles

FMCSA to update the nation's highways to safely incorporate AVs. Already overseeing vehicle certification and the national recall program, NHTSA could conduct the production reviews to ensure that the vehicles are manufactured within a certain tolerance of the original design. While it would be infeasible for any agency to inspect every vehicle manufactured, random spot inspection could provide the information needed to determine the safety of the production process. Finally, for the roadworthiness certification of the vehicle, as they already oversee vehicle safety and issue regulations for truck operations, NHTSA and FMCSA are the logical agencies. NHTSA oversees the FMVSS program and has recall abilities should unsafe conditions be found within the roadworthiness of vehicles.

In response to the ever-changing landscape of air travel, and as technology has changed over the decades, the regulations governing certification have been amended to improve safety. Through this review process, regulations concerning aircraft certification and airworthiness have been amended over 90 times since the 1960s[10]. By updating the safety regulations, the aviation industry has conducted over 90 million successful commercial flights and transported 7.4 billion passengers with just a single fatality over the last decade.

Because the process for aircraft certification and airworthiness is complex and elaborate, the FAA has the authority to designate authorized partners to aid in the process. Starting with the Federal Aviation Act of 1958, FAA activities could be delegated, as necessary, to private individuals employed by the aircraft manufacturers. While on the payroll of the manufacturers, the designated individuals would be the representative for FAA, responsible for overseeing the design work and determining whether the designs were meeting safety requirements [11] . As the aviation industry has expanded, so has the use of delegation within the FAA, with both individuals and organizations being used as delegates to ensure proper safety standards are met. Such individuals and organizations are referred to as *designees*, and are part of the Organization Designation Authorization (ODA) program. The FAA is ultimately responsible for the work performed by the designees[12].

Through the ODA program, designees handle certification of both aircraft and personnel. The ODAs specialize in different certification functions, ranging from initial design and production to certification of airmen and air operators. With respect to aircraft certification, ODAs can be authorized for Type Certification (TC ODA), Supplemental Type Certification (STC ODA), Production Certification (PC ODA), and Parts Manufacturer Certification (PMA ODA). While those designated as a TC ODA can manage and document findings for type certificate programs, and issue airworthiness certificates, they cannot issue original type certificates or amended type certificates, and must have a type certificate before being eligible to be designated an ODA[13]. As of January 2020, 13 organizations hold a TC ODA designation—the majority of which are authorized for other certification capabilities[14]. Overseeing the process of certification, and monitoring the ODAs for compliance with the responsibilities and procedures for aircraft certification, is the Flight Standardization Board (FSB). Unlike the ODA, whose primary objective is to determine the airworthiness and safety of the aircraft for certification, the FSB is responsible for determining the requirements for pilot type ratings, developing training objectives for normal and emergency operations, conducting initial training for pilots and inspectors, and publishing recommendations for use in approving operator training programs[15].

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification

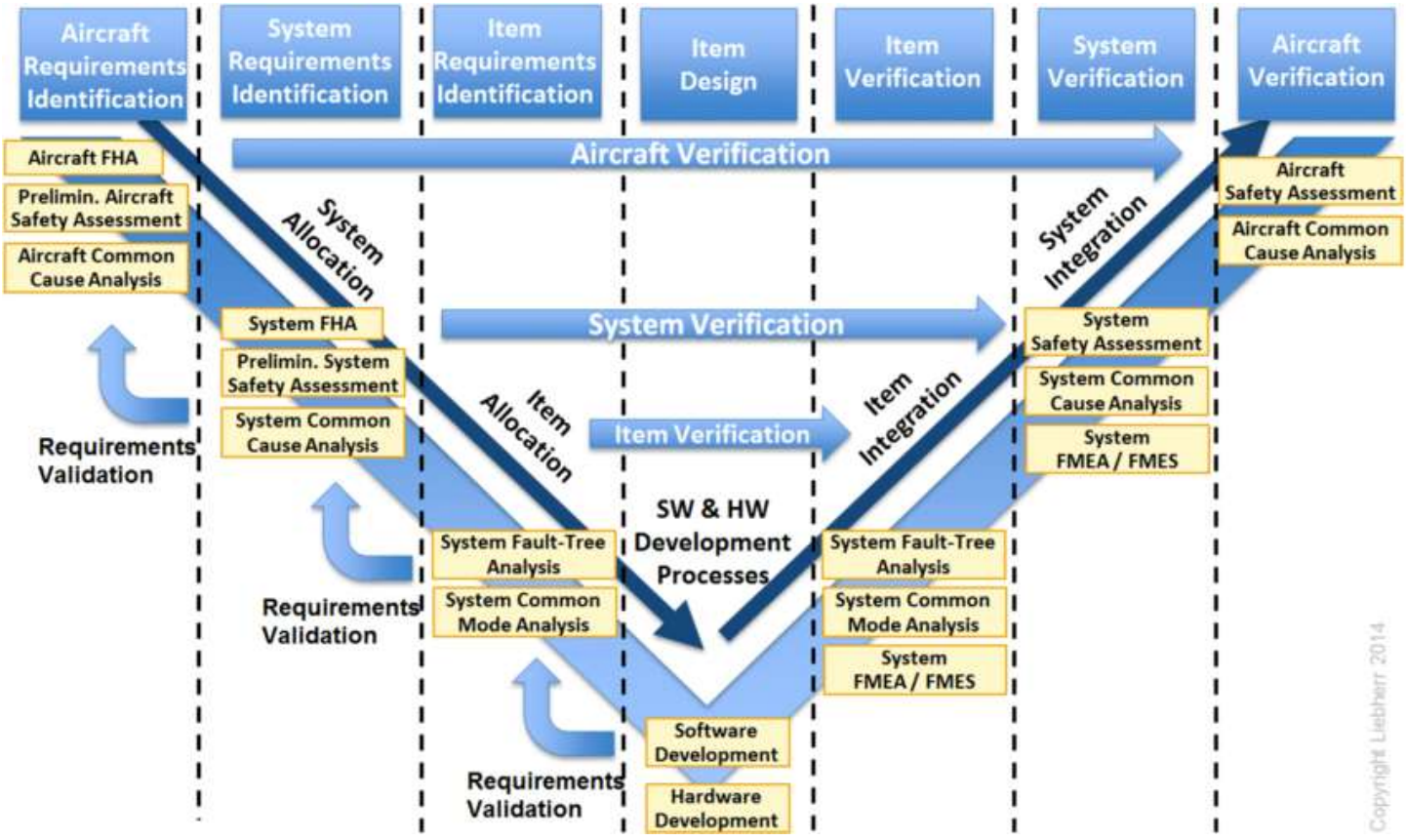


Figure 2: Aviation Systems Certification Model

The assessment and certification processes are extensive and elaborate, which presents both benefits and drawbacks. One benefit is the process outline provided by the FAA in their Order 8110 4C, for those wishing to obtain certification. Along with outlining typical process, the FAA order also discusses the roles and responsibilities of the key players involved in the certification of aircraft. As an extensive number of individuals work on the certification of an aircraft, knowing who is responsible for which functions within the certification process is vital to ensure that the proper information is transmitted to those responsible. Involving ODAs, FSB staff, and FAA engineers in the certification procedures allows for redundancy within the inspection and review process, which can increase the chance that any issues with the design or intended operation can be caught and mitigated.

However, with so many individuals involved, even given the detailed breakdown of roles and responsibilities, confusion can arise in terms of identifying the individual or group (ODA, FSB, or FAA engineers) in charge of a particular task. Such confusion can result in vital safety information being reported to the wrong individual or not reported at all. On top of the unwieldly number of personnel involved, the multiple layers of review can increase the red tape and bureaucracy, which can not only slow down the certification process but also increase the burden of the aircraft manufacturer from both financial and staffing perspectives.

CASE STUDIE

To illustrate the potential risk of failure in current vehicle and aircraft certification programs, two case studies are examined. The first of these studies investigates motor vehicle recalls, highlighting the role of self-certification and the reactive (rather than proactive) response of motor vehicle manufacturers to safety issues. The second of the studies looks into the certification of the Boeing 737 MAX to understand how critical information regarding the safety and autopilot systems was not properly reported to the FAA, and how the certification process may have contributed to these issues.

Automobile Recalls

The last 50+ years have seen major strides in vehicle safety. The National Highway Traffic Safety Administration (NHTSA) reports that 2012 vehicle models on average had a 56% lower fatality rates than comparable models of the 1950s. As safety technology has evolved, the number of safety systems in vehicles has increased to include seatbelts, air bags (front and side), electronic stability control, blind spot detection, and driver assist[16].

The FMVSS were created to govern the performance and safety of vehicle components. Covering the majority of vehicle components, the FMVSS are divided into three categories—crash avoidance, crashworthiness, and post-crash survivability [17]. While NHTSA administers the FMVSS, compliance with the standards is dependent upon a self-certification process, with each manufacturer responsible for their vehicles' compliance with all FMVSS. Upon determining that a vehicle component or completed vehicle meets FMVSS standards, the manufacturer affixes a certification label to the vehicle; Figure 3 provides an example of this label. The label should meet requirements of 49 CFR Part 567 and at a minimum include the vehicle's manufacturer (actual assembler), date of manufacture (month and year), and the following statement: "This vehicle conforms to all applicable Federal motor vehicle safety standards (FMVSS) in effect on the date of manufacture shown above."[18] Because the responsibility to maintain compliance falls on the manufacturers, the response to safety issues is reactive rather than proactive.

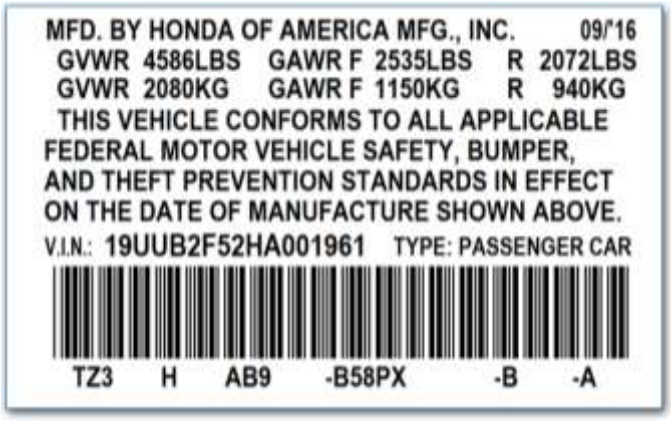


Figure 3: Vehicle Certification Sticker[19] (Source: Automotive ID)

This reactionary approach has led to an increase in recalls, as the current vehicle standards are not able to anticipate or accommodate the impacts of increased technology being placed into new vehicle models. For example, as more electronics have been installed in vehicles, the number of recalls due to electrical and electronic systems has increased, accounting for 6% of recalls in 2015 and resulting in 3 million vehicles recalled in 2017. As electronic systems become ever more vital to vehicles with increased automation, the trend of increasing recalls will continue until more proactive regulations are created. Currently, the number of automobile recalls in all categories are at a 20-year high, with over 1,000 recalls occurring during 2016. Not only has the number of recalls per year increased but also the number of vehicles affected

by each recall, with McKinsey and Company reporting that three cars are recalled for each vehicle sold in 2017[20].

To counteract this trend of increasing vehicle recalls, a thorough review and update of the FMVSS is needed. Recognizing this need, NHTSA has recently conducted a review of the standards, receiving comments and input from professionals across the country. While a review of the FMVSS was performed, the updates are still forthcoming keeping manufacturers as the primary entities to certify their vehicles. With the manufacturers self-certifying their vehicles, more forward-thinking approaches to detection of potential recalls will need to be created.

As the car manufacturers vet and certify their own vehicles, the creation of an inspection program within NHTSA could provide increased oversight. Using inspectors to perform spot checks can potentially catch any issues that arise during a manufacturing process. If issues were to be found, inspectors could then issue recalls before the defects cause adverse operations and fatalities.

Another potential method would be to use simulation and other modeling tools to determine the potential of a recall when a new technology is submitted to the FMVSS. Whether NHTSA does the modeling themselves or relies on the testing that manufacturers conduct during product development, the information gained from these tests can inform NHTSA on the probability of an issue and if a recall is needed. In the future when AVs are more widespread, the recall process could also include the authority of NHTSA to ground AV fleets, similar to FAAs authority when serious design defects are discovered. Recalls not only affect consumers whose vehicles are part of the recall but also negatively impact manufacturers, in terms of both financial losses and decrease in public trust in their brand. In their discussion of recalls, Aragon et al. (2019) rank the types of recalls based on financial impacts—from simple voluntary recalls to NHTSA investigations that involve severe injuries. The latter of these can incur fines up to $1 billion depending

Recalls not only affect consumers whose vehicles are part of the recall but also negatively impact manufacturers, in terms of both financial losses and decrease in public trust in their brand

on the nature and severity of the recall, if the manufacturer can be shown to have known about and concealed potential defects. Along with financial impacts of vehicles recalls, the public perception of a manufacturer can be affected, with the magnitude of impacts varying between companies.

While automakers risk harm to their reputation during recalls, not all brands are affected equally. During the Ford/Firestone recall in 2000–2001, Firestone admitted producing defective tires, but also questioned the vehicle design of the Explorer on which Ford was installing the tires. In their discussion of the recall, the National Automotive Dealers Association (NADA) explains that while the recall and related crashes, injuries, and deaths attained widespread media attention, the impact to Ford's reputation and truck prices was minimal. During and after the recall, the competitiveness of Ford's prices for their used trucks dropped only 2–3%, with prices resuming their upward trend by 2002[21]. In contrast, the series of recalls in 2010 made by Toyota were also highly publicized, with a great deal of negative sentiment expressed on online platforms. Unlike in the case of Ford, Toyota's pricing took a significant hit, dropping from almost 40% higher than their competitors' pricing to just 20%. Once the recalls were over and prices began to stabilize, Toyota recovered some of their edge,

with prices ultimately settling around 30% higher than that of their competitors.

So, what caused such drastically different perception and pricing losses for the two companies? NADA notes that at the time of the recalls, Toyota was known for high quality and reliability, whereas in Ford's case public expectations were low and the brand's value was not at the same level of its competitors[21]. Because of their greater reputation, Toyota had farther to fall than Ford did.

When reviewing the automobile certification process, several pros and cons reveal themselves.

Pros

Baseline safety - The issuance of FMVSS provides a baseline of safety to ensure that the public is not endangered by faulty vehicle products.

Familiarity - The FMVSS have been issued since the late 1960s, so companies are familiar with the standards, which allows for an expedited compliance process.

Cons

Limited oversight - While NHTSA administers the FMVSS, it is up to the motor vehicle companies to certify that each vehicle is compliant with all applicable standards, as NHTSA is not able to test every model or vehicle[22].

Reactionary - The way the FMVSS are written and administered, they are reactionary in nature to new technologies and safety issues rather than being proactive in trying to anticipate safety compliance issues of new technologies.

Competing rating systems – The Insurance Institute for Highway Safety (IIHS) publishes its own rating system for vehicles. Both NHTSA and IIHS rate vehicles based on safety crash testing but use different methods and rating systems, which make comparisons between the two systems difficult. The two systems also do not use speeds in their ratings, and test vehicles below 40 mph in crash testing[22].

Boeing 737 MAX

In response to competition in traditional American markets from competitors, such as Airbus, Boeing in 2011 announced that it would release a new generation of its 737 line of planes. Retaining the wing and body design of its predecessor, the 737NG (where NG stands for "next generation"), the 737 MAX series would incorporate new engines and avionics[23]. The first new 737 MAX began rolling out of the factory at the end of 2015, with the first flight taking place in January of 2016. After a little more than a year of flight testing, the FAA announced the certification of the 737 MAX 8[24].

The 737 MAX retained the body and wing design of the 737NG to allow for quicker certification of the planes and retention of a wider pool of pilots and ground crew experienced in operating the aircraft. However, the new engines for the 737 MAX were positioned further forward than those of the previous generation, leading to nose pitch issues while operating at lower speeds or at increased angles of attack. To correct this pitching issue, Boeing engineers developed the Maneuvering Characteristics Augmentation System (MCAS), which would allow for the automatic swivel of the horizontal tail to move the nose of the plane back down[24]. Even though it was meant to work automatically, MCAS was programmed to work only when the plane was being flown manually, meaning it was not a part of the autopilot systems[23]. Unlike most other safety systems that rely on redundant sensors, the MCAS relied on information from only one angle-of-attack sensor, which was considered

acceptable by Boeing engineers as the chance of critical malfunction by MCAS was extremely unlikely.

Following the flight-testing period of the new plane in 2016, the FAA approved the certification of the 737 MAX 8 in March of 2017. In October of 2018, a Lion Air flight crashed a few minutes after take-off, with pilots reporting "flight control problems," with the nose of plane being forced downward. A review of the events leading up to the crash revealed that during the previous flight, the sensor and avionics were reporting incorrect speeds and altitudes, but the aircraft was kept in service. In response to the scrutiny that the MCAS system and the pilots' reactions to the situation received, Boeing and the FAA released an Airworthiness Directive (AD) advising pilots on how to handle stabilizer control issues. Even with the AD and inspections of 737 MAXs to determine airworthiness, an Ethiopian Airlines flight crashed in March of 2019. This second flight, still under investigation, led to the grounding of all 737 MAX planes worldwide.

Criticism over the MCAS system and its certification has been widespread, with questions surrounding the need for increased pilot training and documentation on MCAS included in operation manuals. As the aircraft body and wings were the same design as the previous generation of 737, it was given the same pilot rating as the previous generations. Due to this similarity, it was determined that pilots would only need to take a tablet-based course rather than train in a simulator, as would be required for new planes. Further criticism arose when documentation for MCAS, which was given more power over the horizontal stabilizer than the original certified by the FAA, was not included in the pilots' training manual[23,24]. While the reasoning behind this decision was that the system worked in the background without pilot control, Boeing expected the pilots to be able to troubleshoot and disable MCAS should it perform abnormally.

Along with the lack of training and materials provided to pilots, the certification of the MCAS system has also received scrutiny. The original version of the MCAS program was designed to work in limited and highly specific situations, in which a high angle-of-attack and excessive g-forces cause non-smooth stick forces for pilots. Boeing's submission to the FAA for certification included analyses of MCAS failure situations to determine the redundancy needs of the sensors. While the aircraft contained two sensors at the time of analysis, it was determined to only need one in flight based on the testing. In the failure analysis presented to the FAA, Boeing found that the likelihood of failure was extremely unlikely, with a failure occurring once every 223 trillion hours of flight (Gates and Baker, 2019). While the initial likelihood of failure was found to be extremely low, after the first crash, internal FAA analysis found a high likelihood of subsequent crashes, estimating 15 over the 30- to 40-year life of the aircraft. However, the planes were allowed to keep flying[23].

This emphasis on safety will be especially important for AVs as the technology involved with their operation is significantly more complex than current vehicles on the road.

Upon further simulation and flight testing, the same non-smooth stick force issue was found at lower speeds. This issue prompted Boeing to expand the authority that MCAS had to control for lower speed conditions. Because g-forces are not excessive at lower speed, the g-force sensor criterion was removed from the software and MCAS could be triggered with just a single sensor input—high angle-of attack. Even though MCAS was given extra control over the horizontal stabilizer, and a sensor input requirement was removed, no new or

updated documentation was sent to the FAA. At the same time, the FAA did not request any of the new safety analysis for these changes as it was not deemed critical, with the critical phase of flight considered to be higher cruise speeds.

Further documentation showed that the failure analyses conducted by Boeing did not consider that MCAS could be triggered repeatedly, nor was the failure of the single input sensor considered—although the failure of the single sensor initiated both the Lion Air and Ethiopian Airline crashes. The single sensor was used as a measure to ensure that the system would work in case either sensor on the plane failed to function. The move to use only a single sensor input was also one of cost savings as the complexity of the system was kept to a minimum. Minimizing complexity allowed for quicker testing, as Boeing was trying to catch up to the Airbus A320[24].

Two lessons learned can be gleaned from the two crashes and subsequent grounding of Boeing's 737 MAX aircraft. The first lesson highlights the need for a renewed emphasis on safety, with redundancy and backup procedures rigorously tested. This emphasis on safety will be especially important for AVs as the technology involved with their operation is significantly more complex than that of current vehicles on the road. This complexity leads to the second lesson learned from the 737 MAX's grounding—in addition to providing proper documentation on control systems, airlines must ensure pilots have sufficient training to attain and maintain the skills needed to operate the aircraft. In the case of AVs, increased instruction prior to obtaining a license may be needed, or the requirement that a certain number of hours a month must be driven manually to ensure driving skills are maintained (similar to pilot requirements for manual flight).

AV SAFETY ASSESSMENT OPPORTUNITIES

As automation continues to increase in automobiles, aviation can provide lessons learned for safety assessment and certification pathways. As automation within aviation increased, the safety standards and assessment procedures were updated in order to continue to ensure the safety of commercial air travel. While the process used in aviation cannot directly be applied to AVs, the procedures used by the FAA and their delegates can be amended for application to AVs.

One of the most important aspects from aviation is the need for strong, **clear standards and safety assessment procedures**. As the central federal agencies regulating automobiles, NHTSA and the Federal Highway Administration would be the logical authorities to provide a nationwide standard for AVs. As TxDOT is responsible for the safety of motorists on Texas roadways, and with the federal agencies hesitating to establish national AV standards (instead relying on the current set of FMVSS), TxDOT could benefit from establishing a state-level roadworthiness program. Such a program could be modeled on the aviation industry's airworthiness certification process, drafting a detailed list of requirements to ensure safe AV operations.

As this white paper highlights, the process to assess and certify the safety of an aircraft is elaborate and involves many individuals. AV certification will be just as elaborate, requiring the review of many systems and components. As such, following the methods used by the FAA, **redundancy in reviews** can allow for the detection of any faults within the design and operation of AVs. This redundancy can ensure that vehicle manufacturers do not self-certify vehicles that have not been fully vetted

against applicable standards. Along with the initial creation and application of standards, a continuous process of **standards review** with amendments is needed to assure the safety of new technologies that are developed after the initial deployment of AVs.

As the aviation industry discovered after the introduction of automation, drivers must have the necessary driving skills to take over in the event of a malfunction; regular practice of manual driving is critical for public safety. This is especially important as vehicles that have increased automated functions, but that are not fully autonomous, are deployed, because the public may misunderstand the level of function that these vehicles have. As the former CEO of Starsky Robotics put it, "supervised machine learning doesn't live up to the hype. It isn't actual artificial intelligence akin to C-3PO, it's a sophisticated pattern-matching tool"[25].

As states oversee licensing and regulation of drivers, it will be up to TxDOT and other state agencies to **develop and update training and licensing materials**. The FAA's FSB program uses 'test subjects' who have not been trained on a particular aircraft before to determine the efficacy of training programs; such an approach could serve as model for training drivers on AV systems. As mentioned above, until AVs are fully autonomous, the driver will need to be aware of the role of the driver and vehicle at each level of automation.

"Supervised machine learning doesn't live up to the hype. It isn't…akin to C-3PO, it's a sophisticated pattern-matching tool."

Guidance for Autonomous Vehicle Safety Evaluation

White Paper

Lessons Learned from Aviation Certification

BIBLIOGRAPHY

[1] US DOT, 2015. Air Commerce Act. Retrieved from https://www.transportation.gov/content/air-commerce-act [Accessed February 6, 2020]

[2] FAA, u.d. FAA Historical Chronology, 1926-1996. Federal Aviation Administration, US DOT. Available at: https://www.faa.gov/about/history/chronolog_history/media/b-chron.pdf [Accessed February 6, 2020]

[3] Little, Becky, 2019. Automation of Planes Began 9 Years After the Wright Bros Took Flight—But It Still Leads to Baffling Disasters. History. Retrieved from https://www.history.com/news/plane-automation-autopilot-flight-302-610 [Accessed February 6, 2020]

[4] Hope, Allison, 2017. How Autopilot on Planes Works. Conde Nast Traveler. Retrieved from https://www.cntraveler.com/story/how-autopilot-on-planes-works [Accessed February 6, 2020]

[5] SKYbrary, 2020. Cockpit Automation- Advantages and Safety Challenges. Retrieved from https://www.skybrary.aero/index.php/Cockpit_Automation_-_Advantages_and_Safety_Challenges# [Accessed February 6, 2020]

[6] FAA, 2017. Order 8110.4C: Type Certification. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8110_4C_Chg_6.pdf [Accessed February 6, 2020]

[7] Auerbach 49 U.S.C. §44704 (2018). Type Certificates, production certificates, airworthiness certificates, and design and production organization certificates. Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2018-title49/pdf/USCODE-2018-title49-subtitleVII-partA-subpartiii.pdf [Accessed February 11, 2020]

[8] FAA, 2005. Condition for Safe Operation. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/aircraft/air_cert/airworthiness_certification/cond_safe_oper/ [Accessed February 11, 2020]

[9] Taibi, D., Lenarduzzi, V., Dieudonne, L., Plociennik, C., 2015. Towards a Classification Schema for Development Technologies: an Empirical Study in the Avionic Domain. Retrieved from https://www.researchgate.net/figure/Avionics-V-Model-extract-from-the-ARP4754A-12_fig1_310776068 [Accessed March 2, 2020]

[10] FAA, 2019a. Aircraft Certification by the Numbers. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/aircraft/air_cert/by_the_numbers/ [Accessed February 11, 2020]

[11] FAA, 2016. Delegation and Designee Background. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/about/history/deldes_background/ [Accessed February 12, 2020]

[12] FAA, 2018. Delegated Organizations. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/other_visit/aviation_industry/designees_delegations/delegated_organizations/ [Accessed February 12, 2020]

[13] FAA, 2019b. Types of Organizational Designation Authorizations. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/other_visit/aviation_industry/designees_delegations/delegated_organizations/types/ [Accessed February 12, 2020]

[14] FAA, 2020. FAA ODA Directory. Federal Aviation Administration, United States Department of Transportation. Retrieved from https://www.faa.gov/other_visit/aviation_industry/designees_delegations/designee_types/media/ODADirectory.pdf [Accessed February 12, 2020]

[15] FAA, 2019c. Flight Standardization Board (FSB). Federal Aviation Administration, United States Department of

Transportation. Retrieved from https://www.faa.gov/aircraft/air_cert/airworthiness_certification/fsb/ [Accessed February 13, 2020]

[16] NHTSA, 2020. Newer Cars are Safer Cars. National Highway Traffic Safety Administration, United States Department of Transportation. Retrieved from https://www.nhtsa.gov/newer-cars-are-safer-cars [Accessed February 7, 2020]

[17] Taylor Auto Glass, 2015. What is FMVSS and Why Does it Matter? Retrieved from https://www.taylorautoglass.com/fmvss-matter/ [Accessed February 10, 2020]

[18] NHTSA, n.d. Importation and Certification FAQs- What certifications are required on motor vehicles? National Highway Traffic Safety Administration, United States Department of Transportation. Retrieved from https://www.nhtsa.gov/importing-vehicle/importation-and-certification-faqs-8 [Accessed March 4, 2020]

[19] Automotive ID, n.d. Label Samples-Certification. Retrieved from https://www.automotiveid.com/Label-Samples.aspx [Accessed March 4, 2020]

[20] Aragon, Adriana, Ulrich Huber, Timo Moller, and Heiko Nick. "Return to Sender: Resolving the Automotive-Recall Resurgence." McKinsey & Company, February 2019. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/return-to-sender-resolving-the-automotive-recall-resurgence.

[21] NADA, 2014. The Impact of Vehicle Recalls on the Automotive Market. National Automotive Dealers Association. Retrieved from https://www.autonews.com/Assets/pdf/NADA%20UCG_WhitePaper_Impact%20of%20Vehicle%20Recalls.pdf [Accessed February 10, 2020]

[22] DeVeau, DJ., 2016. NHTSA & IIHS Pros and Cons. Medium. Retrieved from https://medium.com/@daviddeveau/nhtsa-iihs-pros-cons-fe3cba149e30 [Accessed February 10, 2020]

[23] Slotnick, David, 2019. Boeing CEO Dennis Muilenburg is out as the 737 Max crisis drags on. Here's the complete history of the plane that's been grounded since 2 crashes killed 346 people 5 months apart. Business Insider. Retrieved from https://www.businessinsider.com/boeing-737-max-timeline-history-full-details-2019-9 [Accessed February 19, 2020]

[24] Gates, D., and Baker, M., 2019. The inside story of MCAS: How Boeing's 737 MAX system gained power and lost safeguards. The Seattle Times. Retrieved from https://www.seattletimes.com/seattle-news/times-watchdog/the-inside-story-of-mcas-how-boeings-737-max-system-gained-power-and-lost-safeguards/ [Accessed February 19, 2020]

[25] Seltz-Axmacher, S., 2020. The End of Starsky Robotics. Retrieved from https://medium.com/starsky-robotics-blog/the-end-of-starsky-robotics-acb8a6a8a5f5 [Accessed August 05, 2020]